Tampereen yliopisto

Emma Takku

FERMAT'N SUURI LAUSE EKSPONENTILLE NELJÄ

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Joulukuu 2019

Tiivistelmä

Emma Takku: Fermat'n suuri lause eksponentille neljä
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Joulukuu 2019

Tutkielmassa käsitellään Fermat'n suurta lausetta ja erityisesti Fermat'n suurta lausetta eksponentille neljä, joka todistetaan käyttäen äärettömän laskeutumisen menetelmää. Tätä todistusta varten tutkielmassa käsitellään myös aritmetiikan peruslausetta sekä Pythagoraan kolmikoita. Tutkielma sisältää muutamia esimerkkejä näistä aiheista. Pythagoraan kolmikoihin liittyen käsitellään muun muassa kolmikon jäsenten jaottomuutta sekä Pythagoraan kolmikon primitiivisyyttä.

Tutkielmassa käydään läpi myös Fermat'n suuren lauseen historiaa. Tutkielmassa käydään läpi todistuksen historiaan liittyviä henkilöitä ja kerrotaan heidän saavutuksistaan todistuksen saralla.

Avainsanat: Fermat'n suuri lause, Fermat'n suuri lause eksponentille neljä ja Pythagoraan kolmikot

Sisältö

1 Johdanto

Tässä tutkielmassa tarkastellaan *Fermat'n suurta lausetta* ja erityisesti sen todistusta, kun eksponentti on neljä. Fermat'n suuri lause eksponentille neljä todistetaan luvussa 4 käyttämällä äärettömän laskeutumisen menetelmää. Todistus on itsensä Fermat'n kehittämä.

Luvun 3 alaluvussa 3.1 todistetaan *aritmetiikan peruslause*, jonka mukaan jokainen yhtä suurempi positiivinen kokonaisluku voidaan kirjoittaa yksikäsitteisenä alkulukujen tulona. Alaluvussa esitellään myös aritmetiikan peruslauseen yhteys suurimman yhteisen tekijän määrittämiseen. Aiheita avataan esimerkkien avulla.

Fermat'n suuren lauseen neljännen eksponentin tapauksen todistusta varten alaluvussa 3.2 määritellään *Pythagoraan kolmikko* ja käydään läpi sen ominaisuuksia, kuten Pythagoraan kolmikon primitiivisyys, sen jäsenten jaottomuus sekä jäsenten parillisuus ja parittomuus. Luvun 4 kannalta merkittävä on erityisesti lause 3.7, jossa muodostetaan primitiivisen Pythagoraan kolmikon jäsenten lausekkeet. Tässä hyödynnetään aritmetiikan peruslausetta.

Luvussa 2 käydään läpi Fermat'n suuren lauseen vaiherikasta historiaa 1600-luvulta tähän päivään. Luvussa esitellään joitakin varhaisia tuloksia Fermat'n suureen lauseeseen liittyen ja mainitaan merkittävimpiä lausetta tutkineita matemaatikoita. Heitä ovat muun muassa Euler, Germain sekä Kummer. Luvussa kerrotaan myös Fermat'n suuren lauseen todistamisen saamasta huomiosta mediassa, mikä on matemaatisille löydöille harvinaista.

Lukijalta edellytetään yliopistomatematiikan alkeiden hallintaa. Lukijan odotetaan ymmärtävän esimerkiksi alkuluvun käsite, jaollisuuden käsite ja siihen liittyviä tuloksia, algebrallista yhtälönratkaisua sekä induktioperiaate. Päälähteinä käytetään K. Rosenin teosta Elementary Number Theory and Its Applications ja D. Burtonin teosta Elementary Number Theory. Lisäksi lähteenä on käytetty P. Ribenboimin teosta 13 Lectures on Fermat's Last Theorem.

2 Historiaa

Matemaatikko ja tuomari Pierre de Fermat kirjoitti arvioilta vuonna 1637 muistiinpanojensa marginaaliin vapaasti suomennettuna:

> On mahdotonta kirjoittaa kuutiota kahden kuution summana, neljättä potenssia kahden neljännen potenssin summana tai ylipäätään mitään potenssia kahden kyseessä olevan potenssin summana. Olen löytänyt tähän kerrassaan loistavan todistuksen, mutta marginaali on liian pieni sen kirjoittamiseksi.

Tästä saadaan *Fermat'n suuri lause*, jonka mukaan Diofantoksen yhtälöllä $x^n+y^n = z^n$ ei ole rakaisuja, kun eksponentti n on suurempi tai yhtä suuri kuin kolme ja muuttujat x, y ja z ovat nollasta poikkeavia kokonaislukuja. Fermat'n muistiinpanojen marginaalissa mainittua todistusta ei kuitenkaan koskaan löydetty. [1, s. 234.] Fermat onnistui kuitenkin todistamaan tapauksen eksponentti $n = 4$ [4, s.488]. Lauseen todistaminen ehti haastaa matematiikoita yli 350 vuoden ajan. Vuonna 1908 saksalainen teollisuusjohtaja Paul Wolfskehl jopa lupasi Fermat'n suuren lauseen todistajalle sadan tuhannen markan palkkion. Tämä kuitenkin johti vain tuhansien virheellisten todistusten julkaisemiseen. Kun toimiva todistus kaikille mahdollisille potensseille n viimein löytyi vuonna 1995, uutinen levisi mediassa laajalle, mikä on matematiikkaan liittyville uutisille harvinaista. Kyseessä siis todella oli merkittävä matemaattinen löytö. [4, s. 488, 491 – 492.]

Moni matemaatikko epäonnistui yrittäessään todistaa Fermat'n suurta lausetta, mutta yritysten ansiosta syntyi uusia matematiikan osa-alueita, kuten elliptiset käyrät ja rengasteoria. Ensimmäinen merkittävä edistysaskel lauseen todistuksessa saavutettiin vuonna 1770, kun Euler todisti tapauksen $n = 3$. Tästä todistuksesta kuitenkin löydettiin pian virhe, mutta Legendre onnistui paikkamaan sen. Tiettyjen eksponentin n tapausten todistamisen sijaan ranskalainen matemaatikko Sophie Germain keskittyi lauseen todistamiseen yleisemmällä tasolla. Vuonna 1805 hän osoitti, että jos p ja $2p + 1$ ovat alkulukuja, yhtälöllä $x^p + y^p = z^p$ ei ole ratkaisuja kokonaislukumuuttujilla x, y ja z, kun kyseiset muuttujat ovat erisuuria kuin nolla ja kun $p \nmid x$, $p \nmid y$ ja $p \nmid z$. Lisäksi Germain osoitti, että yhden muuttujista x, y, z on oltava jaollinen viidellä, jos $x^5 + y^5 = z^5$. Vuonna 1825 Dirichlet ja Legendre täydensivät todistuksen Fermat'n suuren lauseen tapaukselle $n = 5$. He käyttivät todistuksessa

äärettömän laskeutumisen menetelmää, jota myös itse Fermat käytti todistaessaan tapauksen $n = 4$. Lamé todisti samalla menetelmällä tapauksen $n = 7$, neljätoista vuotta myöhemmin vuonna 1839. [4, s. 488.]

1800-luvun puolivälissä eri matemaatikot lähestyivät Fermat'n suuren lauseen todistusta uusistä näkökulmista, mutta eniten edistystä sai aikaan saksalainen Ernst Kummer, joka onnistui todistamaan lauseen pätevyyden kaikilla sataa pienemmillä kokonaislukupotensseilla, lukuunottamatta tapauksia $n = 37$, $n = 59$ ja $n = 67$. Tämä todistus synnytti paljon algebrallisen lukuteorian tutkimusta, mikä johti abstraktiin algebraan kuuluvan rengasteorian syntyyn. Saksalainen Gerd Faltings teki vuonna 1986 ensimmäisen havainnon Fermat'n suuren lauseen ja elliptisten käyrien yhteydestä. Lisäksi Faltings osoitti, että yhtälöllä $x^n + y^n = z^n$ on rajallinen määrä nollasta eroavia kokonaislukuratkaisuja. Tämä määrä olisi pitänyt osoittaa nollaksi, kun eksponentti $n \geq 3$, jotta Fermat'n suuri lause oltaisiin saatu todistettua. [4, s. 488 – 490.] Loogikot yrittivät laatia pätevää todistusta lähestymällä ongelmaa aksioomien kautta, mutta tuloksetta [3, s. 216].

Teknologian kehittyessä saatiin kehitettyä useita tietokoneohjelmia, jotka testasivat, toteutuuko Fermat'n suuri lause muuttujan n eri arvoilla. Vuoteen 1977 mennessä Sam Wagstaff oli tällaisten ohjelmien avulla osoittanut lauseen pätevyyden potensseille $n \leq 125000$ ja vuoteen 1993 menessä eri ohjelmien avulla oli osoitettu lauseen pätevyys kaikille potensseille neljään miljoonaan saakka. Kuitenkaan todistusta Fermat'n suurelle lauseelle ei ollut näkyvissä. [4, s. 490.]

Vuosisatoja pohditun ongelman ratkaisi viimein Princetonin yliopiston professori Andrew Wiles. Hän kiinnostui Fermat'n suureesta lauseesta lukiessaan siitä vuonna 1963 olessaan vasta kymmenvuotias ja kertomansa mukaan tiesi jo silloin, ettei voisi luovuttaa kuuluisan, monia matemaatikoita haastaneen ongelman suhteen. Wiles tutki vuosien ajan elliptisiä käyriä, mikä myöhemmin auttoi Fermat'n suuren lauseen todistuksen kehittämisessä. Kun Wiles huomasi olevansa toimivan todistuksen jäljillä, hän hylkäsi kaiken muun tutkimustyönsä ja keskittyi vain todistuksen kehittämiseen. Todistustyönsä ensimmäisinä vuosina Wiles puhui aiheesta kollegoidensa kanssa, mutta totesi keskusteluiden häiritsevän työtään. [4, s. 490 – 491.]

Vuonna 1993 Wiles todisti Fermat'n suuren lauseen luentosarjansa aikana Cambridgen yliopistossa. Seitsemän vuoden intensiivisen työn tuloksena syntyneessä todistuksessa hän käytti hyvin monimutkaisia elliptisiin käyriin liittyviä metodeja ja monet nimekkäät matemaatikot olivat vaikuttuneita. Tieto kuuluisan ongelman ratkaisemisesta levisi ympäri maailman. Todistusta tarkemmin tutkittaessa siitä kui-

tenkin löydettiin merkittävä ongelma, jonka epäiltiin olevan ratkaisematon. Jo vuotta myöhemmin Wiles kuitenkin onnistui kollegansa Taylorin avustuksella korjaamaan virheen. Lopulta vuonna 1995 Wiles julkaisi toimivan 125 sivua pitkän todistuksen Fermat'n suurelle lauseelle. Wilesille myönnettiin useita palkintoja työstään, kuten Wolfskehlin aikanaan lupaama rahapalkkio Göttingenin Tiedeakatemian myötämänä. Saatuaan vuosien työn onnistuneesti päätökseen Wiles sai viimein mielenrauhan. [4, s. 490 – 492.]

3 Valmistelevia tarkasteluja

3.1 Aritmetiikan peruslause

Aritmetiikan peruslause on tärkeä lukuteorian tulos, jonka todistamiseen tarvitaan apulauseita 3.1 ja 3.2.

Apulause 3.1. Olkoot a, b ja c positiivisia kokonaislukuja, joilla lukujen a ja b suurin yhteinen tekijä on 1, eli $\text{syt}(a, b) = 1$, ja $a \mid bc$, eli a jakaa lukujen b ja c tulon. Tällöin $a \mid c$.

Todistus. [4, s. 97.] Koska $\text{syt}(a, b) = 1$ on olemassa kokonaisluvut x ja y, joilla $ax + by = 1$. Kerrottaessa yhtälön molemmat puolet muuttujalla c saadaan $acx + bcy = c$. Nyt siis $a \mid acx+bcy$, koska $a \mid a$, $a \mid bc$ ja $acx+bcy$ on näiden lineaarikombinaatio. Näin ollen $a \mid c$. □

Apulause 3.2. Olkoon p alkuluku ja olkoot $a_1, a_2, \ldots, a_n$ positiivisia kokonaislukuja. Jos $p \mid a_1a_2 \ldots a_n$, on olemassa kokonaisluku i, $1 \leq i \leq n$, jolla $p \mid a_i$.

Todistus. [4, s. 97.] Todistetaan apulause induktiolla.

Tapaus $n = 1$ on selvästi tosi.

Oletetaan, että lause on tosi indeksille n. Pidetään $n+1$ luvun tuloa $a_1a_2 \ldots a_{n+1}$ jaollisena alkuluvulla p. Nyt koska $p \mid a_1a_2 \ldots a_{n+1} = (a_1a_2 \ldots a_n)a_{n+1}$, $p \mid a_1a_2 \ldots a_n$ tai $p \mid a_{n+1}$. Jos $p \mid a_1a_2 \ldots a_n$, induktio-oletuksen perusteella on olemassa kokonaisluku i, $1 \leq i \leq n$, jolla $p \mid a_i$. Näin ollen $p \mid a_i$ jollakin kokonaisluvulla i, $1 \leq i \leq n+1$.

Lause on siis induktioperiaatteen nojalla tosi. □

Nyt voidaan todistaa aritmetiikan peruslause. Todistus koostuu kahdesta osasta. Ensin osoitetaan, että jokainen yhtä suurempi positiivinen kokonaisluku voidaan esittää ainakin yhdellä tavalla alkulujen tulona, eli sille on olemassa ainakin yksi alkulukuhajotelma. Toiseksi osoitetaan, että näitä alkulukuhajotelmia on vain yksi jokaista yhtä suurempaa positiivista kokonaislukua kohti. [4, s. 97.]

Lause 3.3. ***Aritmetiikan peruslause*** *Jokainen yhtä suurempi positiivinen kokonaisluku voidaan kirjoittaa yksikäsitteisenä alkulujen tulona, eli alkulukuhajotelmana. Alkulukutekijät kirjoitetaan kasvavaan järjestykseen.*

Todistus. [4, s. 97 – 98.] Osoitetaan ensin vastaoletuksen avulla, että jokainen yhtä suurempi positiivinen kokonaisluku voidaan kirjoittaa alkulukujen tulona.
Oletetaan, että on olemassa positiivisia kokonaislukuja, joita ei voida esittää alkulujen tulona. Olkoon n pienin tällainen kokonaisluku. Jos n on alkuluku, sillä on selvästi alkulukuhajotelma. Kokonaisluku n ei siis voi olla alkuluku. Olkoon $n = ab$, missä $1 < a < n$ ja $1 < b < n$. Nyt koska a ja b ovat pienempiä kuin n, niiden on oltava alkulukujen tuloja. Täten myös n on alkulukujen tulo, sillä $n = ab$. Tämä ristiriita osoittaa, että kaikki yhtä suuremmat positiiviset kokonaisluvut voidaan kirjoittaa alkulukujen tulona.
Osoitetaan vielä, että positiivisten kokonaislukujen alkulukuhajotelmat ovat yksikäsitteisiä.
Oletetaan, että on olemassa kokonaisluku n, jolla on kaksi erilaista alkulukuhajotelmaa. Olkoon siis

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t,$$

jossa $p_1, p_2, \dots p_s$ ja $q_1, q_2, \dots q_t$ ovat alkuluja, joilla $p_1 \leq p_2 \leq \cdots \leq p_s$ ja $q_1 \leq q_2 \leq \cdots \leq q_t$. Poistetaan yhtälöstä kaikki sen molemmilla puolilla alkuluvut. Tällöin saadaan yhtälö

$$p_{i_1} p_{i_2} \dots p_{i_u} = q_{j_1} q_{j_2} \dots q_{j_v},$$

jonka eri puolilla ei ole samoja alkuluja ja jossa $u \geq 1$ ja $v \geq 1$. Apulauseen 3.2 mukaan $p_{i_1} \mid q_{j_k}$ jollakin muuttujan k arvolla. Tämä on kuitenkin mahdotonta, sillä jokainen q_{j_k} on alkuluku ja eroaa alkuluvusta p_{i_1}. Syntyy ristiriita, minkä seurauksena alkuperäinen väite on tosi. Positiivisten kokonaislukujen alkulukuhajotelmat ovat siis yksikäsitteisiä. □

Positiivisen kokonaisluvun n alkulukuhajotelma kertoo olennaista tietoa kyseisestä kokonaisluvusta. Alkulukuhajotelman avulla voidaan esimerkiksi nähdä, jakaako alkuluku p kokonaisluvun n, sillä $p \mid n$, jos ja vain jos p esiintyy sen alkulukuhajotelmassa. Esimerkiksi koska $168 = 2^3 \cdot 3 \cdot 7$, alkuluvut 2, 3 ja 7 jakavat luvun 168 ja esmierkiksi alkuluvut 5, 11 tai 17 eivät. Lisäksi alkuluvun p korkein potenssi, joka jakaa kokonaisluvun n, on alkuluvun p potenssi myös kokonaisluvun n alkulukuhajotelmassa. Toisin sanoen kokonaisluku d jakaa kokonaisluvun n, jos ja vain jos kaikki alkuluvut kokonaisluvun d alkulukuhajotelmassa esiintyvät kokonaisluvun n alkulukuhajotelmassa vähintään yhtä suurina potensseina kuin kokonaisluvun d hajotelmassa. [4, s. 98 – 99.]

Esimerkki 3.1. Lukujen 52, 215 ja 468 alkulukuhajotelmat ovat

$$52 = 2 \cdot 2 \cdot 13 = 2^2 \cdot 13, 215 = 5 \cdot 43, 468 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 13 = 2^2 \cdot 3^2 \cdot 13.$$

Esimerkki 3.2. Koska $120 = 2^3 \cdot 3 \cdot 5$, luvun 120 positiiviset alkulukutekijöitä ovat alkulukuhajotelman luvut 2, 3 ja 5 yhtä suurilla tai pienemmillä potensseilla kuin alkulukuhajotelmassa. Luvun 120 positiiviset kokonaislukutekijät ovat siis

1	3	5	$3 \cdot 5 = 15$
2	$2 \cdot 3 = 6$	$2 \cdot 5 = 10$	$2 \cdot 3 \cdot 5 = 30$
$2^2 = 4$	$2^2 \cdot 3 = 12$	$2^2 \cdot 5 = 20$	$2^2 \cdot 3 \cdot 5 = 60$
$2^3 = 8$	$2^3 \cdot 3 = 24$	$2^3 \cdot 5 = 40$	$2^3 \cdot 3 \cdot 5 = 120$

[4, s. 99.]

Alkulukuhajotelmia voidaan käyttää myös suurimman yhteisen tekijän etsimiseen. Merkitään luvuista a ja b pienempää merkinnällä $\min(a, b)$. Olkoot lukujen a ja b alkulukuhajotelmat

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n},$$

joissa jokainen eksponentti on epänegatiivinen kokonaisluku ja joissa kaikki lukujen a ja b hajotelmissa esiintyvät alkuluvut kuuluvat molempiin hajotelmiin. Huomataan, että

$$\text{syt}(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)},$$

[4, s. 99.] Havainnollistetaan tätä esimerkin avulla.

Esimerkki 3.3. Lukujen 720 ja 2100 alkulukuhajotelmat ovat

$$720 = 2^4 \cdot 3^2 \cdot 5, 2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7.$$

Näiden lukujen suurimman yhteisen tekijän alkulukuhajotelma voi siis sisältää vain alkuluvut 2, 3 ja 5, eivätkä näiden alkulukujen potenssit voi olla suurempia kuin niiden potenssit lukujen 720 ja 2100 alkulukuhajotelmissa. Näin ollen $\text{syt}(720, 2100) = 2^2 \cdot 3 \cdot 5 = 60$. [4, s. 99.]

3.2 Pythagoraan kolmikot

Pythagoraan lauseen mukaan kolmion kateettien pituuksien neliöiden summa on kolmion hypotenuusan pituuden neliö. Kolmen positiivisen kokonaisluvun joukkoja, jotka yhdessä toteuttavat tämän ehdon, kutsutaan Pythagoraan kolmikoiksi. Nimitykset on annettu kreikkalaisen matemaatikon Pythagoraan mukaan. [4, s. 482].

Määritelmä 3.1. Olkoot x, y ja z positiivisia kokonaislukuja ja toteuttakoot ne yhtälön

$$x^2 + y^2 = z^2.$$

Tällöin kolmikkoa x, y, z kutsutaan *Pythagoraan kolmikoksi*. [4, s. 482].

Esimerkki 3.4. Kolmikot 3, 4, 5 ja 12, 35, 37 ovat Pythagoraan kolmikoita [1, s. 235], koska $3^2 + 4^2 = 25 = 5^2$ ja $12^2 + 35^2 = 1369 = 37^2$.

Pythagoraan kolmikoiden toteuttama yhtälö on kahden muuttujan Diofantoksen yhtälö, eli kokonaislukukertoiminen polynomiyhtälö, jossa on vähintään kaksi muuttujaa ja jolle etsitään kokonaislukuratkaisuja. [4, s. 481]. Käydään seuraavaksi läpi muutamia Pythagoraan kolmikoihin liittyviä ominaisuuksia.

Määritelmä 3.2. Pythagoraan kolmikko x, y, z on *primitiivinen*, jos muuttujien x, y, z suurin yhteinen tekijä on 1, eli

$$\text{syt}(x, y, z) = 1$$

[4, s. 482].

Huomionarvoista on, että kaikki primitiivisen Pythagoraan kolmikon parit ovat keskenään jaottomia. Tätä ominaisuutta hyödynnetään lauseen 3.7 todistuksessa. [1, s. 236].

Määritelmä 3.3. Kokonaisluvut a ja b ovat *keskenään jaottomia*, jos niiden suurin yhteinen tekijä on 1, eli

$$\text{syt}(a, b) = 1$$

[4, s. 80].

Apulause 3.4. Jos Pythagoraan kolmikko (x, y, z) on primitiivinen, niin

$$\text{syt}(x, y) = \text{syt}(x, z) = \text{syt}(y, z) = 1$$

Todistus. [4, s. 483.] Oletetaan, että x, y, z on Pythagoraan kolmikko ja että $\text{syt}(x, y) > 1$. Olkoon p alkuluku ja $p \mid \text{syt}(x, y)$. Nyt siis $p \mid x$ ja $p \mid y$. Tämän perusteella tiedetään, että $p \mid (x^2 + y^2) = z^2$. Koska $p \mid z^2$ voidaan päätellä, että $p \mid z$. Tämä on kuitenkin ristiriita, sillä kolmikon x, y, z ollessa primitiivinen Pythagoraan kolmikko $\text{syt}(x, y, z) = 1$, jolloin $\text{syt}(x, y) = 1$. Samoin voidaan todistaa, että $\text{syt}(x, z) = \text{syt}(y, z) = 1$. □

Apulause 3.5. Olkoon x, y, z primitiivinen Pythagoraan kolmikko. Tällöin toinen muuttujista x ja y on parillinen ja toinen pariton.

Todistus. [1, s. 236.] Jos muuttujat x ja y ovat molemmat parillisia, $2 \mid (x^2 + y^2)$ eli $2 \mid z^2$ eli $2 \mid z$. Tällöin $\text{syt}(x, y, z) \geq 2$, mikä Pythagoraan kolmikon primitiivisyyden nojalla on kuitenkin epätosi. Molemmat muuttujat x ja y eivät siis voi olla parillisia. Jos x ja y taas olisivat molemmat parittomia, niin $x^2 \equiv 1 \pmod 4$ ja $y^2 \equiv 1 \pmod 4$, siis

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

Tämä on kuitenkin epätosi, sillä kokonaisluvun neliö on aina kongruentti luvulle 0 tai 1 modulo 4. Näin ollen toisen muuttujista x ja y on oltava parillinen ja toisen pariton. □

Apulauseesta 3.5 nähdään, että ei ole olemassa primitiivistä Pythagoraan kolmikkoa, jonka jokainen muuttuja x, y ja z olisi alkuluku. Kuitenkin muuttuja z ja jompi kumpi muuttujista x ja y voivat olla alkulukuja. Tällaisia kolmikoita ovat esimerkiksi 3, 4, 5 ja 19, 180, 181. [1, s.236.]

Lauseessa 3.7 hyödynnetään Aritmetiikan peruslauseeseen pohjautuvaa apulausetta 3.6, jonka mukaan kahden keskenään jaottoman positiivisen kokonaisluvun tulon ollessa neliö, myös kyseiset kokonaisluvut ovat neliöitä.

Apulause 3.6. Olkoot r, s ja t positiivisia kokonaislukuja ja olkoot $\text{syt}(r, s) = 1$ ja $rs = t^2$. Tällöin on olemassa kokonaisluvut m ja n, joilla $r = m^2$ ja $s = n^2$.

Todistus. [4, s. 484.] Tapaus $r = 1$, $s = 1$ on selvästi tosi. Voidaan siis olettaa, että $s > 1$ ja $r > 1$. Olkoot muuttujien r, s ja t alkulukuhajotelmat

$$\begin{aligned} r &= p_1^{a_1} p_2^{a_2} \dots p_u^{a_u}, \\ s &= p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \dots p_v^{a_v}, \\ t &= q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}. \end{aligned}$$

Nyt koska $\text{syt}(r, s) = 1$, lukujen r ja s alkulukuhajotelmissa esiintyvät eri alkuluvut. Oletuksen mukaan $rs = t^2$, eli saadaan

$$p_1^{a_1} p_2^{a_2} \dots p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \dots p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} \dots q_k^{2b_k}$$

Aritmetiikan peruslauseen nojalla yllä olevan yhtälön eri puolilla olevat alkulujen potenssit ovat samoja. Siis jokainen alkuluku p_i vastaa alkulukua q_j jollakin muuttujan j arvolla toisiaan vastaavilla eksponenteilla, jolloin $a_i = 2b_j$. Täten siis jokainen eksponentti a_i on parillinen ja edelleen $a_i/2$ on kokonaisluku. Nyt $r = m^2$ ja $s = n^2$, kun muuttujat m ja n ovat kokonaislukuja

$$m = p_1^{a_1/2} p_2^{a_2/2} \dots p_u^{a_u/2}$$

ja

$$n = p_{u+1}^{a_{u+1}/2} p_{u+2}^{a_{u+2}/2} \dots p_v^{a_v/2}.$$

□

Nyt voidaan todistaa tulos, joka antaa kaikki primitiiviset Pythagoraan kolmikot.

Lause 3.7. *Olkoot x, y ja z positiivisia kokonaislukuja. Muuttujat x, y ja z muodostavat primitiivisen Pythagoraan kolmikon, jossa y on parillinen, jos ja vain jos on olemassa keskenään jaottomat positiiviset kokonaisluvut m ja n, joilla $m > n$, m on pariton ja n parillinen tai m on parillinen ja n pariton ja joilla*

$$\begin{aligned} x &= m^2 - n^2, \\ y &= 2mn, \\ z &= m^2 + n^2. \end{aligned}$$

Todistus. [4, s. 484 – 486.] Olkoon kolmikko x, y, z primitiivinen Pythagoraan kolmikko. Osoitetaan, että on olemassa lauseessa määritellyt kokonaisluvut m ja n.

Koska oletuksen mukaan y on parillinen, apulauseen 3.5 mukaan x on pariton ja tämän seurauksena myös z on pariton. Näin ollen $z + x$ ja $z - x$ ovat parillisia, joten luvut $r = (z + x)/2$ ja $s = (z - x)/2$ ovat kokonaislukuja.

Koska $x^2 + y^2 = z^2$, saadaan $y^2 = z^2 - x^2 = (z + x)(z - x)$. Siispä

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = rs.$$

Olkoon $\text{syt}(r, s) = d$. Nyt koska $d \mid r$ ja $d \mid s$, $d \mid (r + s) = z$ ja $d \mid (r - s) = x$. Siis $d \mid \text{syt}(x, z) = 1$ eli $d = 1$ eli $\text{syt}(r, s) = 1$.

Apulauseen 3.6 perusteella on olemassa positiiviset kokonaisluvut m ja n, joilla $r = m^2$ ja $s = n^2$. Kun x, y ja z kirjoitetaan muuttujien m ja n avulla, saadaan

$$\begin{aligned} x &= r - s = m^2 - n^2, \\ y &= \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn, \\ z &= r + s = m^2 + n^2. \end{aligned}$$

Nyt $\text{syt}(m, n) = 1$, sillä jokaisen muuttujien m ja n yhteisen jakajan on jaettava myös $x = m^2 - n^2$, $y = 2mn$ sekä $z = m^2 + n^2$ ja tiedetään, että $\text{syt}(x, y, z) = 1$. Huomataan myös, että m ja n eivät voi olla samanaikaisesti parittomia. Jos näin olisi, x, y ja z olisivat kaikki parillisia. Tämä ei ole mahdollista, sillä $\text{syt}(x, y, z) = 1$. Nyt koska $\text{syt}(m, n) = 1$ ja molemmat muuttujat m ja n eivät voi olla parittomia, m on parillinen ja n pariton tai toisinpäin. Siispä jokaisella primitiivisellä Pythagoraan kolmikolla on lauseessa esitetty muoto.

Todistuksen viimeistelyksi on vielä osoitettava, että jokainen kolmikko

$$\begin{aligned} x &= m^2 - n^2, \\ y &= 2mn, \\ z &= m^2 + n^2, \end{aligned}$$

jossa m ja n ovat positiivisia kokonaislukuja, $m > n$, $\text{syt}(m, n) = 1$ ja $m \not\equiv n \pmod 2$, muodostaa primitiivisen Pythgoraan kolmikon.

Ensin huomataan, että kolmikko $m^2 - n^2$, $2mn$, $m^2 + n^2$ muodostaa Pythagoran kolmikon, koska

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 \\ &= (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2 \\ &= z^2. \end{aligned}$$

Jotta tämä Pythagoraan kolmikko olisi primitiivinen, on osoitettava, että muuttujien x, y ja z arvot ovat keskenään jaottomia. Olkoon $\text{syt}(x, y, z) = d > 1$. Tällöin on olemassa alkuluku p, jolla $p \mid \text{syt}(x, y, z)$. Huomataan, että $p \neq 2$, sillä muuttuja x on pariton. Lisäksi, koska $p \mid x$ ja $p \mid z$, $p \mid (z + x) = 2m^2$ ja $p \mid (z - x) = 2n^2$. Nyt siis $p \mid m$ ja $p \mid n$. Tästä seuraa ristiriita, sillä tiedetään, että $\text{syt}(m, n) = 1$. Siispä $\text{syt}(x, y, z) = d = 1$, eli kolmikko x, y, z muodostaa primitiivisen Pythagoraan kolmikon. □

Seuraavassa esimerkissä käydään läpi, miten lausetta 3.7 voidaan hyödyntää primitiivisten Pythagoraan kolmikoiden etsinnässä.

Esimerkki 3.5. Olkoon $m = 7$ ja $n = 2$. Nyt $m > n$, $\text{syt}(m, n) = 1$ ja $m \not\equiv n \pmod 2$, eli lauseen 3.7 ehdot toteutuvat. Siispä saadaan

$$x = m^2 - n^2 = 7^2 - 2^2 = 49 - 4 = 45,$$
$$y = 2mn = 2 \cdot 7 \cdot 2 = 28,$$
$$z = m^2 + n^2 = 7^2 + 2^2 = 49 + 4 = 53.$$

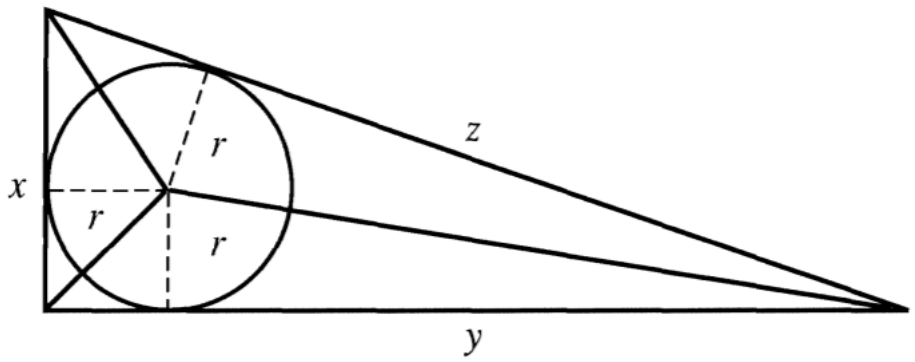
Selvästi 45, 28 ja 53 ovat positiiviisia kokonaislukuja, joten lauseen 3.7 nojalla kolmikko 45, 28, 53 on primitiivinen Pythagoraan kolmikko.

Esimerkkki 3.5 osoittaa, että primitiivisten Pythagoraan kolmikoiden etsintä ei vaadi pitkiä tai monimutkaisia laskutoimituksia, jos voidaan hyödyntää lausetta 3.7.

Suorakulmaista kolmiota, jonka sivujen pituudet ovat kokonaislukuja, kutsutaan *Pythagoraan kolmioksi*. Pyhagoraan kolmioista on tehty mielenkiintoinen geometrinen löytö.

Lause 3.8. *Pythagoraan kolmion sisään piirretyn ympän säde on aina kokonaisluku.*

Todistus. [1, s. 238 – 239.] Olkoon Pythagoraan kolmion hypotenuusa z, kateettien pituudet x ja y ja olkoon kolmion sisään piirretyn ympyrän säde r. Pythagoraan kolmio voidaan jakaa kolmeen kolmioon. Kaikkien kolmen kolmion korkeus on r ja kantojen pituudet ovat x, y ja z. Tätä havainnollistetaan alla olevassa kuvassa 3.1.



Kuva 3.1. Pythagoraan kolmion pinta-alan määritys [2, s. 250].

Koska kolmion pinta-ala määritetään jakamalla kannan ja korkeuden tulo kahdella, Pythagoraan kolmion pinta-alaksi saadaan

$$\frac{1}{2}xy = \frac{1}{2}rx + \frac{1}{2}ry + \frac{1}{2}rz = \frac{1}{2}r(x + y + z).$$

Nyt siis $x^2 + y^2 = z^2$. Tämän yhtälön positiiviset kokonaislukuratkaisut saadaan lausekkeista

$$\begin{aligned} x &= k(m^2 - n^2) \\ y &= 2kmn \\ z &= k(m^2 + n^2) \end{aligned}$$

kun valitaan sopivat kokonaisluvut m, n ja k. Nyt jos lausekkeeseen $xy = r(x+y+z)$ sijoitetaan muuttujien x, y ja z paikalle niille annetut lausekkeet, saadaan säteeksi

$$\begin{aligned} r &= \frac{k(m^2 - n^2)2kmn}{k(m^2 - n^2) + 2kmn + k(m^2 + n^2)} \\ r &= \frac{2k^2mn(m^2 - n^2)}{k((m^2 - n^2) + 2mn + (m^2 + n^2))} \\ r &= \frac{2k^2mn(m^2 - n^2)}{k(2mn + m^2 - n^2 + m^2 + n^2)} \\ r &= \frac{2k^2mn(m^2 - n^2)}{k(2mn + 2m^2)} \\ r &= \frac{2kmn(m^2 - n^2)}{2m(n + m)} \\ r &= \frac{kn(m^2 - n^2)}{(m + n)} \\ r &= \frac{kn((m + n)(m - n))}{(m + n)} \\ r &= kn(m - n), \end{aligned}$$

joka on kokonaisluku. Näin ollen Pythagoraan kolmion, jonka sivujen pituudet ovat kokonaislukuja, sisälle piirretyn ympyrän säde on aina kokonaisluku. □

4 Fermat'n suuri lause

Alaluvussa 3.2 käsiteltiin yhtälöä $x^2+y^2 = z^2$. Pierre de Fermat kuitenkin tutki lausetta myös suuremmilla eksponenteilla. Tämä tunnetaan *Fermat'n suurena lauseena*. Tämän lauseen yleinen todistus sisältää hyvin monimutkaista ja hienostunutta matematiikkaa, joka ylittää tämän tutkielman tason.

Lause 4.1. ***Fermat'n suuri lause*** *Olkoot muuttujat x, y ja z nollasta eroavia kokonaislukuja ja* $n \geq 3$*. Tällöin Diofantoksen yhtälöllä*

$$x^n + y^n = z^n$$

ei ole ratkaisuja. [4, s. 488.]

4.1 Eksponentti neljä

Vaikka Fermat ei koskaan ainakaan tiedettävästi onnistunut todistamaan lausetta 4.1, hän kuitenkin todisti lauseen tapauksen $n = 4$. Todistuksessa käytetään Fermat'n kehittelemää äärettömän laskeutumisen menetelmää, joka pohjautuu positiivisten kokonaislukujen joukon olemassaolevaan alarajaan. Menetelmässä oletetaan, että lauseelle olisikin olemassa ratkaisu positiivisilla kokonaisluvuilla. Tämä ratkaisu kuitenkin luo uuden ratkaisun vielä pienemmillä positiivisilla kokonaisluvuilla ja uusi vastaus luo jälleen uuden ratkaisun edelleen pienemmillä positiivisilla kokonaisluvuilla ja niin edelleen. Tätä vastausten ketjua voitaisiin siis jatkaa loputtomiin. Tämä ei kuitenkaan ole mahdollista, sillä positiivisten kokonailukujen joukko on alhaalta rajoitettu. Syntyy siis ristiriita, mikä todistaa alkuperäisen väitteen, että kokonailukuratkaisuja ei ole, todeksi. [1, s. 241.]

Todistamalla, että Diofantoksen yhtälöllä $x^4 + y^4 = z^2$ ei ole ratkaisuja positiivisilla kokonaisluvuilla, saadaan samalla todistettua Fermat'n suuren lauseen tapaus $n = 4$, sillä $x^4 + y^4 = z^4 = (z^2)^2$ [4, s. 492]. Todistetaan siis Fermat'n suuri lause eksponentille neljä todistamalla lause 4.2.

Lause 4.2. *Diofantoksen yhtälöllä*

$$x^4 + y^4 = z^2$$

ei ole ratkaisuja nollasta poikkeavilla kokonaisluvuilla x, y ja z.

Todistus. [4, s. 492 – 494.] Oletetaan, että yhtälöllä on olemassa ratkaisu nollasta poikkeavilla kokonaisluvuilla x, y ja z. Koska negatiivisen kokonaisluvun neljäs potenssi on aina positiivinen, voidaan olettaa, että kokonaisluvut x, y ja z ovat positiivisia.

Oletetaan myös, että $\text{syt}(x, y) = 1$. Tämän osoittamiseksi olkoon $\text{syt}(x, y) = d$ ja olkoot $x = dx_1$ ja $y = dy_1$, joissa x_1 ja y_1 ovat positiivisia kokonaislukuja. Olkoon lisäksi $\text{syt}(x_1, y_1) = 1$. Nyt koska $x^4 + y^4 = z^2$, saadaan

$$(dx_1)^4 + (dy_1)^4 = z^2$$

ja edelleen

$$d^4(x_1^4 + y_1^4) = z^2.$$

Näin ollen $d^4 \mid z^2$, eli $d^2 \mid z$. Siispä on olemassa positiivinen kokonaisluku z_1, jolla $z = d^2 z_1$. Nyt siis

$$d^4(x_1^4 + y_1^4) = (d^2 z_1)^2 = d^4 z_1^2,$$

eli

$$x_1^4 + y_1^4 = z_1^4.$$

Yhtälön $x^4 + y^4 = z^2$ rakaisuksi saadaan siis positiiviset kokonaisluvut $x = x_1$, $y = y_1$ ja $z = z_1$, joilla $\text{syt}(x_1, y_1) = 1$. Näin ollen $d = 1$, eli $\text{syt}(x, y) = 1$.

Oletetaan, että yhtälöllä $x^4 + y^4 = z^4$ on ratkaisu $x = x_0$, $y = y_0$, $z = z_0$, jossa x_0, y_0 ja z_0 ovat positiivisia kokonaislukuja ja joilla $\text{syt}(x_0, y_0) = 1$. Osoitetaan nyt, että yhtälölle on olemassa toinen ratkaisu positiivisilla kokonaisluvuilla $x = x_1$, $z = z_1$ ja $z = z_1$, joilla $\text{syt}(x_1, y_1) = 1$ ja $z_1 < z_0$. Nyt koska $x_0^4 + y_0^4 = z_0^2$, saadaan

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2,$$

joten kolmikko x_0^2, y_0^2, z_0 on Pythagoraan kolmikko. Lisäksi $\text{syt}(x_0^2, y_0^2) = 1$, koska jos on olemassa alkuluku p, jolla $p \mid x_0^2$ ja $p \mid y_0^2$, niin $p \mid x_0$ ja $p \mid y_0$. Tämä on ristiriidassa sen kanssa, että $\text{syt}(x_0, y_0) = 1$. Siispä $\text{syt}(x_0^2, y_0^2) = 1$, minkä seurauksena kolmikko x_0^2, y_0^2, z_0 on primitiivinen Pythgoraan kolmikko. Lauseen 3.7 mukaan on siis olemssa positiiviset kokonaisluvut m ja n, joilla $\text{syt}(m, n) = 1$, $m \not\equiv n \pmod 2$ ja

$$\begin{aligned} x_0^2 &= m^2 - n^2, \\ y_0^2 &= 2mn, \\ z_0 &= m^2 + n^2, \end{aligned}$$

jossa muuttuja y_0^2 on valittu parilliseksi. Lausekkeista saadaan

$$x_0^2 + n^2 = m^2.$$

Nyt, koska $\text{syt}(m, n) = 1$, kolmikko x_0, n, m on primitiivinen Pythagoraan kolmikko, m on pariton ja n on parillinen. Jälleen lauseen 3.7 mukaan on olemassa positiiviset kokonaisluvut r ja s, joilla $\text{syt}(r, s) = 1$, $r \not\equiv s \pmod 2$ ja

$$x_0 = r^2 - s^2,$$
$$n = 2rs,$$
$$m = r^2 + s^2.$$

Muuttujat m ollessa pariton ja $\text{syt}(m, n) = 1$ tiedetään, että $\text{syt}(m, 2n) = 1$. Koska $y_0^2 = (2n)m$, apulauseen 3.6 mukaan on olemassa positiiviset kokonaisluvut z_1 ja w, joilla $m = z_1^2$ ja $2n = w^2$. Lisäksi, koska w on parillinen, $w = 2v$, missä v on positiivinen kokonaisluku, jolla

$$v^2 = n/2 = rs.$$

Nyt koska $\text{syt}(r, s) = 1$, apulauseen 3.6 mukaan on olemassa positiiviset kokonaisluvut x_1 ja y_1, joilla $r = x_1^2$ ja $s = y_1^2$. Huomataan myös, että koska $\text{syt}(r, s) = 1$, myös $\text{syt}(x_1, y_1) = 1$.

Näin ollen saadaan yhtälö

$$x_1^4 + y_1^4 = r^2 + s^2 = m = z_1^2,$$

jossa muuttujat x_1, y_1 ja z_1 ovat positiivisia kokonaislukuja ja joilla $\text{syt}(x_1, y_1) = 1$. Lisäksi $z_1 < z_0$, sillä

$$z_1 \leq z_1^4 = m^2 < m^2 + n^2 = z_0.$$

Oletus siis oli, että yhtälöllä $x^4 + y^4 = z^2$ on ainakin yksi kokonaislukuratkaisu. Nyt tiedetään, että positiivisten kokonaislukuratkaisujen joukossa on olemassa muuttujan z pienin arvo z_0. Edellä on kuitenkin osoitettu, että tämän ratkaisun z_0 avulla voidaan löytää uusi ratkaisu pienemmällä muuttujan z arvolla, mikä johtaa riistiriitaan. Näin ollen lause on todistettu äärettömän laskeutumisen menetelmällä. □

Seuraus 4.3. *Yhtälöllä $x^4 + y^4 = z^4$ ei ole positiivisia kokonaislukuratkaisuja.*

Todistus. [1, s. 242.] Jos yhtälöllä $x^4+y^4 = z^4$ olisi positiivinen kokonaislukuratkaisu muuttujilla x_0, y_0, z_0, muuttujat x_0, y_0, z_0^2 toteuttaisivat yhtälön $x^4 + y^4 = z^2$, mikä ei lauseen 4.1 nojalla ole mahdollista. Siispä yhtälöllä $x^4 + y^4 = z^4$ ei ole positiivisia kokonaislukuratkaisuja. □

Lähteet

[1] Burton, D. *Elementary Number Theory*. 5. p. New York: McGraw-Hill, Yhdysvallat. 2002.

[2] Burton, D. *Elementary Number Theory*. 6. p. New York: McGraw-Hill, Yhdysvallat. 2007.

[3] Ribenboim, P. *13 Lectures on Fermat's Last Theorem* New York: Springer-Verlag, Yhdysvallat. 1979.

[4] Rosen, K. *Elementary Number Theory and Its Applications*. 4. p. Addison-Wesley, Yhdysvallat. 2000.